GOLDMAN JUDIN INC.
ATTORNEYS
Reg No. 1998/011/368/21

2nd Floor, North Block
Thrupps Illovo Centre
204 Oxford Road Illovo 2196

PO Box 78662 Sandton 2146
Docex 264 Randburg

e-mail: law@elawnet.co.za
website : www.gji.co.za
tel : (+27 11) 268 0287
fax : (+27 11) 268 0282

Cyberliability Policies against Cybersecurity Incidents

Johannesburg, 15 March 2013 - In their excellent article Adrian Azer and Miriam Smolen of the Washington, DC law firm of Gilbert LLP wrote as follows: "On February 12, 2013, President Obama issued an executive order detailing his plan to improve critical infrastructure cybersecurity.

[1] See Executive Order – Improving Critical Infrastructure Cybersecurity, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

(February 12, 2013). In the Executive Order, President Obama notes that it is the policy of the United States to "maintain a cyber environment that encourages efficiency, innovation, and economic prosperity . . . ." The Executive Order states that this policy can be achieved "through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

More specifically, the Executive Order calls for the development of a Cybersecurity Framework by the Director of the National Institute of Standards and Technology. The Cybersecurity Framework will provide "a set of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks" and "shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."

Although the Executive Order requires owners and operators of critical infrastructure to adopt the Cybersecurity Framework, other entities may also be required to adopt the

framework. Section 8 of the Executive Order establishes "a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities." Further, the Executive Order provides that sector-specific agencies may "develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."

We do not yet know which sector-specific agencies will adopt the Cybersecurity Framework, but both the Securities and Exchange Commission and the Federal Trade Commission have already been active in the cybersecurity area. In 2011, the Securities and Exchange Commission provided guidance regarding the disclosure requirements for public companies arising from cybersecurity risks. Meanwhile, the Federal Trade Commission has actively prosecuted several actions within the last year against various companies based on their alleged failure to maintain appropriate cyber-security measures. Given these agencies' interest in cybersecurity, it seems likely that they will be among the sector-specific agencies that consider requiring regulated entities to implement the Cybersecurity Framework.

Even if a company is not currently considered part of critical infrastructure, the Executive Order acts as fair warning that cybersecurity regulation is soon coming. Moreover, with the imposition of regulation, there likely will be increasing private litigation against companies that experience a cybersecurity incident, with the potential for significant losses resulting from governmental fines or damages awarded in litigation.

Companies should act now to protect themselves from such losses, including examining their insurance portfolios to ensure that adequate insurance coverage currently exists. If a company does not have stand-alone coverage for cyber risk, companies should highly consider acquiring cyberliability policies that can protect against either third-party or first-party losses, or both. Third-party cybersecurity policies may provide coverage for:

1. liability for permitting access to identifying information of customers;
2. transmitting a computer virus or malware to a third-party customer or business partner;
3. failing to notify a third party of their rights under the relevant regulations in the event of a security breach; and

4. potential “advertising injury,” i.e., harms through the use of electronic media, such as unauthorized use or infringement of copyrighted material, as well as libel, slander, and defamation claims.

First-party cybersecurity policies may provide coverage for:

1. the costs of providing notice to individuals whose identifying information was compromised;
2. the costs associated with determining the scope of the breach and taking steps to stop the breach;
3. public relations services to counteract the negative publicity that can be associated with a data investigation;
4. the costs of responding to government investigations;
5. the costs of replacing damaged hardware or software;
6. the costs of responding to parties vandalizing the company’s electronic data; and
7. business interruption costs.

Moreover, cybersecurity insurance coverage is in its infancy and there has not been the standardization of policy language. Accordingly, negotiation of policy language is possible and critical.

[1] The Executive Order defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

The above article is of critical interest and importance to South African entities. Improving critical infrastructure cybersecurity is as important in South Africa as it is in the United States of America and elsewhere in the world. Very few South African entities have such cover and it is a sad reflection of South African business that many companies have no idea what is contained in their insurance policies often leaving this very important issue in the hands of their insurance brokers. Competent as the insurance broker may be, it is incumbent upon the directors and prescribed officers of all entities to ensure that the entity has proper and adequate insurance cover and that they fully understand the nature, extent and import of such cover. This is a critical issue for the Risk Committee of an entity and all those involved in risk issues within an entity. Failure to do so will be a breach of the duties imposed upon them in terms of South Africa’s Companies Act and they will also be in breach

of the principles contained in the King Code and Report which applies to all entities on an apply or explain basis. There can also be liability at common law where there has been negligence in this regard. It is vital for such persons to not only ensure that there is adequate and proper cover as required but that they fully understand all of the risks against which the entity is insured and that a proper analysis has revealed that those are the only risks that require cover.

The above article sets out clearly the cyberrisk coverage which is required and it is respectfully recommended that each and every entity consult urgently with their insurance brokers in this regard. The matter should also receive the urgent focus and attention of those persons in the entity responsible for insurance and, as stated above, the matter should also be on the agenda for the risk committee. The matter should be fully ventilated at Board level.

In their excellent article What to Expect When Applying for Cyberinsurance Judy Selby and Brian Esser, a partner and an associate respectively, at Baker Hostetler wrote: “It seems that everyone these days, from President Obama to Facebook account holders, is concerned about cybersecurity. Data breaches and cyberintrusions are front page news, and businesses are warned to take a "when, not if" approach to these threats.

In light of this reality of modern life, more and more businesses are treating data security as one of their most important business risks, and a growing number of insurance companies are offering policies to help businesses prevent and respond to data breaches and attacks. Cyberinsurance policies generally provide both first-party and third-party coverage for such risks. First-party protections include the costs of a forensic investigation to uncover and remediate the breach, retention of privacy lawyers to ensure compliance with relevant laws and regulations, public relations experts to mitigate reputational damage, and companies to notify affected parties of the breach and to conduct credit monitoring, if required. Third-party coverage includes the defense of lawsuits and payment of damages, and coverage for regulatory actions in connection with a security failure, privacy breach, or the failure to disclose a security failure or privacy breach.

While cyberinsurance is not a replacement for diligent in-house data security policies and procedures, prudent businesses should seriously consider it as part of their risk management program. In fact, even the process of applying for cyberinsurance can serve as a useful road map for a business to improve its data security processes.

The policy application

There are a variety of different cyberinsurance products on the market, each with its own unique policy application. Different applications and underwriting standards may be employed depending on the insurer, the applicant's size and industry and the type, quality, and quantity of confidential data it handles and/or maintains.

As with any type of business insurance application, cyberinsurance applications seek general financial information about the prospective insured, including business assets and revenues, number of employees, and anticipated merger and acquisition activity. But cyberinsurance applications delve deeply into other specific areas of the applicant's business that directly impact its data security risk, including the following.

Management of confidential or private information

Applicants often are asked about the volume and types of data they handle and/or maintain. For example, does the company deal with credit/debit card data, Social Security numbers, employee and human resources information, banking/financial records, or medical information? How many confidential records are maintained? Does the company have written, attorney approved policies and procedures concerning the handling of private information? How often are they updated? Is the company compliant with security standards implemented by the credit card industry? Does the company annually assess its compliance with state and federal regulatory standards, such as the Health Insurance Portability and Accountability Act and Graham-Leach-Bliley Act? Does the company employ a chief privacy officer?

Computer systems and network

Cyberinsurance applicants are asked about their existing network security program, including the use of firewalls, antivirus software, programs to test and audit network security controls, network intrusion testing procedures, and the use of remote access to their computer network. They can be asked if they employ a chief information or chief technology officer. Insurers will want to know about the applicant's encryption policies, backup procedures, and the existence of disaster recovery plans. If the applicant utilizes an outside vendor or consultant to manage its computer system and network, the insurer may inquire into their qualifications, processes, and procedures. In light of the trend towards

"bring your own device" programs, insurers want to know if systems are in place to secure mobile devices that have access to business data.

For policies with business interruption coverage, insurers also ask about the volume of sales transacted online on an hourly basis during a normal business day. Applicants with networked point-of-sale systems, such as computer registers and kiosks, may be asked about their average sales per hour.

Employees

Insurers often ask about the applicant's pre-employment screening procedures, such as criminal background checks and drug testing. They also inquire as to the applicant's written security training policies and procedures and if/how they are distributed to employees, policies for creating and updating passwords and termination of computer access as part of the business's regular employee exit processes.

Business partners

If the applicant shares confidential information with other companies, insurers will want to know if those business partners are required to demonstrate adequate security, indemnify the company for data breaches, and maintain their own insurance for breaches.

Websites

If the company maintains a website, insurers are likely to ask who has access to it, whether it is used to conduct transactions using credit cards or online bill payment, what type of information is available from it, and whether the contents are screened by an attorney for disparagement and copyright infringement issues.

Prior incidents

Insurers typically inquire about the prospective insured's three-to-five year history with regard to any actual or alleged failure to prevent unauthorized access to private information. The applicant will be asked to provide information concerning the nature of the event, including whether it was caused by a company insider or a third party, and any associated costs and damages. Some insurers ask how much time elapsed between the

breach and its discovery, and how long it took to resolve the problem after the breach was discovered.

Insurers may ask if the company has been threatened with extortion, such as a threat to disable the company's computer network or website if certain demands are not met. Applicants also will be asked to disclose any denial of service attacks or known intrusions into their computer system. In addition, insurers want to know if the applicant currently is aware of any facts or circumstances that reasonably could give rise to a claim under prospective policy. Some insurers also ask if any other insurer has canceled or refused to renew a cyberinsurance policy within the past few years.

Conclusion

It is unlikely that a single department of a company can complete the typical cyberinsurance application. The team required to do so will likely cut across legal, human resources, compliance, risk, internal audit, and technology departments. The applicant's CIO, CTO, and/or CPO should be involved at the earliest phases of the application process. Inquires directed towards compliance with HIPAA, GLBA, and other data protection standards will require the assistance of the compliance or legal departments.

Cyberinsurance applications often call for the applicant's president, CEO, or CIO to sign the application and declare that the information being submitted is true and correct to the best of their knowledge, and that every reasonable effort has been made to facilitate the proper and correct completion of the application. The applicant also is required to notify the insurer of any application changes prior to the issuance of the policy. Great care should be taken in connection with the completion of the application because it will become a part of the cyberinsurance policy itself, if it is issued. Depending on the circumstances, incorrect information submitted in the application may become an issue if a claim is tendered for coverage under the policy.

Once the application is submitted, for smaller risks the insurer may simply provide a quote for the coverage. Larger risk applicants should expect to receive some follow-up questions from the insurer. Due to the variety and complexity of the various policies on the market, cyberinsurance applicants are urged to work with experienced professionals to ensure that they obtain the best coverage for their particularized needs.”

Prepared by J. Michael Judin

Michael expresses his gratitude to Adrian Azer and Miriam Smolen of the Washington, DC law firm of Gilbert LLP and to Judy Selby and Brian Esser of Baker Hostetler for kindly and generously allowing him to quote from their excellent articles in the preparation of this article.